A group of people posing for the camera

Description automatically generated

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

Versão 1.1

**ÍNDICE**

1. Sobre esta política

2. Objetivo

3. Escopo

4. Princípios Fundamentais de Todas as Políticas

5. Estrutura da Política e Aprovação

5.1. Estrutura

5.2. Aprovação

5.3. Aprovação de Padrões e Política Subordinada

5.4. Revisão Periódica e Nova Aprovação

6. Responsabilidades e Organização

7. Conformidade e Execução

8. Exceções

Apêndice I – Segurança da Informação e Gestão de Risco

Apêndice II – Controle de Documento

**1. SOBRE ESTA POLÍTICA**

Práticas maduras de segurança da informação e gerenciamento de risco da informação estão se tornando cada vez mais importantes para as operações da Onze MC e para a competitividade de mercado da empresa. Falhas de segurança podem comprometer nossa capacidade e confiança de fornecer serviços, podem fazer com que a Onze MC perca receita por meio de fraude ou destruição de dados proprietários ou confidenciais, ou podem fazer com que a Onze MC viole contratos comerciais. Essas falhas podem resultar na perda de segredos comerciais, privacidade de colaboradores e privacidade do cliente. Qualquer uma dessas falhas, particularmente se evidente para o comércio, reduziria a credibilidade e a reputação com os clientes e parceiros da Onze MC.

Para reduzir o risco de tais falhas, a gestão executiva da Onze MC assumiu um forte compromisso de preservar a confidencialidade, integridade e disponibilidade das informações gerenciadas pela Onze MC e mantidas em nome de clientes, colaboradores, investidores, parceiros de negócios, fornecedores e agências governamentais.

Este documento define os princípios e requisitos fundamentais ("Políticas") do Programa de Gerenciamento de Risco e Segurança da Informação da Onze MC ("Programa"), ambos projetados para equilibrar os objetivos, riscos e custos de negócios da Onze MC. Este documento estabelece o escopo dos ativos de informação sujeitos à conformidade com o Programa, atribui funções e responsabilidades para desenvolver, implementar e cumprir esses requisitos e prescreve a aplicação. As Políticas são estruturadas de forma a permitir que a Onze MC aumente a maturidade de suas práticas de gestão de riscos e segurança ao longo do tempo, de acordo com as exigências do mercado e realidades financeiras.

**2. OBJETIVO**

As políticas e sua implementação são projetadas para servir a dois propósitos:

**Segurança** - Reduz o risco de danos à confidencialidade, integridade ou disponibilidade das informações da Onze MC e ativos de tecnologia da informação.

**Conformidade** - Atenda aos requisitos regulamentares e do cliente. Esses requisitos podem exigir conformidade com uma variedade de regulamentos (por exemplo, LGPD) ou estruturas (por exemplo, ISO 27001).

**3. ESCOPO**

Esta Política e todos os seus documentos e componentes relacionados cobrem a Tecnologia Onze MC, que é definida como hardware, software, dispositivos, configurações e serviços de Internet e serviços de terceiros (incluindo todas as formas de serviços em nuvem) projetados para criar, receber, armazenar, processar e transmitir informações.

Esta Política e todos os seus documentos relacionados cobrem e protegem os Dados Corporativos e Pessoais da Onze MC, que são compostos por todos os dados armazenados e gerenciados pela área de Tecnologia Onze MC, sejam dados estratégicos e operacionais da empresa e propriedade intelectual, dados de colaboradores, dados de fornecedores, dados de clientes ou dados governamentais. Esta Política cobre os dados da Onze MC em todas as suas formas, em todas as mídias, durante todas as fases de seu ciclo de vida, incluindo coleta, armazenamento, compartilhamento, uso e destruição.

Esta Política e todos os seus documentos relacionados se aplicam a todos os diretores, executivos, sócios, colaboradores, contratantes independentes, consultores, temporários e estagiários da Onze MC (coletivamente

“Colaboradores”) e colaboradores de empresas terceiras que fazem negócios com a Onze MC, incluindo clientes e fornecedores. Elementos desta política e documentos relacionados aplicam-se a Afiliados e Parceiros.

**4. PRINCÍPIOS FUNDAMENTAIS DE TODAS AS POLÍTICAS**

Os seguintes princípios são fundamentais para a Segurança da Informação e Gestão de Riscos na Onze MC:

Abordagem Baseada em Risco, exceto quando um requisito de conformidade legal dita certas medidas, políticas e sua implementação serão escolhidas para equilibrar

• Os riscos inerentes que existem com a situação atual;

• O custo de remediar e a redução de risco alcançada;

• Necessidades de negócios.

A Separação das Funções de Controle ou direitos de acesso será distribuída para garantir que nenhuma pessoa tenha um conflito de interesses em suas funções ou a capacidade de comprometer um processo crítico.

Indivíduos terão os privilégios de sistema mínimos exigidos para desempenhar suas funções, mas não mais.

Necessidade de Saber, os indivíduos só terão acesso às informações de que precisam para desempenhar suas funções.

**5. ESTRUTURA DA POLÍTICA E APROVAÇÃO**

5.1 Estrutura

As Políticas e padrões de implementação de políticas relacionados (Padrões de Política ou simplesmente “Padrões”) devem ser organizados e estruturados de forma modular para permitir uma revisão e aprovação rápida e eficaz e para tornar mais fácil para aqueles que devem cumprir encontrar a referência apropriada.

Este documento de política é a política de segurança, que inclui os elementos comuns à todas as políticas de segurança.

As políticas de segurança tópicos são políticas subordinadas sobre tópicos específicos; cada um deve ser considerado uma extensão da Política de Segurança Mestre. Essas políticas subordinadas devem incluir outras políticas de governança, políticas que tratem do acesso e uso de ativos de informação com foco nos negócios, e políticas que sejam puramente técnicas. O índice de políticas deve mostrar todas essas políticas completas ou pretendidas, seu estado de revisão e aprovação e a data de sua última aprovação. O Índice também pode ser usado para mostrar quais políticas são necessárias para a conformidade com grupos de ativos de tecnologia específicos (por exemplo, aplicativos voltados para o cliente) ou estruturas de conformidade (por exemplo, conformidade ISO 27001, ISO 27002).

Os padrões de implementação de políticas (“Padrões”) devem ser usados para explicar como as políticas são implementadas.

**5.2 Aprovação**

Esta Política de Segurança da Informação e outras políticas de risco e segurança de informações que tratam da governança devem ser aprovadas pelo Gestor de TI e Segurança da Informação da Onze MC ou seu delegado.

A Gestora Administrativo/Financeiro deve revisar a Política de Segurança da Informação e as políticas subordinadas relacionadas à governança e, mediante acordo, deve apresentar sua recomendação para aprovação da Alta Administração. A Alta Administração deve incluir representantes de Recursos Humanos ou outros indivíduos que possam representar essas funções. A associação deve ser aprovada por altos executivos da Onze MC.

**5.3 Aprovação de Padrões e Política Subordinada**

As políticas temáticas subordinadas que tratam do acesso com foco nos negócios e do uso de ativos de informação devem ser aprovadas pela Alta Administração. Essas políticas devem ser elaboradas com a orientação do Gesto de TI e Segurança da Informação e Gestora Administrativa e Financeira, refletindo as perspectivas das Linhas de Serviço e Divisões e aprovadas para apresentação à Alta Administração.

As políticas de tópico que são exclusivamente de natureza técnica devem ser aprovadas pelo Responsável pela área de Tecnologia. Essas políticas devem ser elaboradas com a orientação da Gestora Administrativo Financeiro.

As normas devem ser aprovadas pela Alta Administração.

**5.4 Revisão Periódica e Nova Aprovação**

Esta Política, seus Padrões, controles relacionados e os procedimentos de suporte devem ser revisados pelo menos uma vez por ano para garantir que eles reduzam o risco de forma útil, atendam aos requisitos de conformidade e segurança, reflitam a organização atual e as realidades comerciais e sejam eficazes em sua implementação.

**6. RESPONSABILIDADES E ORGANIZAÇÃO**

**Profissional TI e Segurança da Informação** – responsável pela implementação de medidas de Segurança da Informação e Gerenciamento de Riscos.

• O Profissional SI pode ter direitos delegados para aprovar políticas, conforme determinado pela alta administração;

• O Profissional SI também é responsável por garantir a implementação das Políticas de Segurança e os Padrões, práticas, controles e procedimentos relacionados.

O Profissional SI é responsável por projetar, organizar, implementar, medir e liderar o Programa de Segurança da Informação e Gerenciamento de Risco, conforme descrito no Apêndice I. Também é responsável pela gestão de riscos e ameaças, sendo necessário projetar, implementar e medir essa gestão. O Profissional SI deverá trabalhar em conjunto com a equipe de Recursos Humanos para promover treinamentos referente à segurança da informação e políticas aplicáveis.

Todos os usuários dos ativos de tecnologia da Onze MC e dados são responsáveis por manter a segurança da tecnologia e dos dados tratados. Aqueles com acesso à tecnologia e dados da Onze MC devem cumprir a Política de Uso Adequado. Os usuários devem cumprir outras políticas específicas com base em suas funções e responsabilidades. Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizados pela Onze MC. Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Onze MC. Descarte adequado de documentos de acordo com seu grau de classificação.

A Equipe de Tecnologia tem responsabilidades adicionais com base em seu acesso adicional à Tecnologia e Dados da Onze MC. Eles devem cumprir todas as políticas pertinentes, incluindo esta política de segurança da informação e todas as políticas subordinadas, padrões de política, linhas de base, etc.

Fornecedores e terceiros que não atuam em funções de cliente, que têm acesso à tecnologia e dados da Onze MC ou fornecem tecnologia à Onze MC, devem concordar por escrito que atenderão a todas as políticas de Segurança da Informação da Onze MC apropriadas.

Clientes com acesso aos dados alojados na tecnologia da Onze MC devem cumprir quaisquer requisitos especiais de segurança e privacidade negociados em contratos.

Afiliados / Parceiros que têm acesso à tecnologia Onze MC ou aos dados da Onze MC devem cumprir a política de segurança da informação que se aplicam às suas circunstâncias.

Utilização da rede interna da Onze MC Consultoria é devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minimizados.

1. A Internet cabeada estará disponível somente para máquinas e equipamentos de propriedade da Onze MC, com a finalidade restrita à realização de atividades inerentes ao desempenho de tarefas de seus colaboradores;

2. A Internet sem fim (wifi) é segregada, garantindo o isolamento da rede interna da Onze MC, com objetivo de fornecer acesso a sistemas e dados internos apenas para os colaboradores desempenharem suas tarefas; existem outras redes com acesso apenas à Internet disponibilizadas à visitantes e usuários que não precisam/podem ter acesso aos dados internos;

3. O Departamento Pessoal é responsável por notificar/comunicar formalmente a Equipe de Tecnologia sobre desligamentos de colaboradores e prestadores de serviços temporários ou terceirizados, para que os acessos sejam revogados;

4. A Onze MC reserva-se o direito de monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos;

5. Os equipamentos, tecnologias e serviços fornecidos para acesso à Internet são de propriedade da Onze MC, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação;

6. A Internet disponibilizada pela Onze MC aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que seja autorizada e não prejudique o andamento dos trabalhos nos setores/unidades;

7. É proibida a divulgação e/ou compartilhamento indevido de informações internas, confidenciais e confidenciais restritas em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que use a Internet como via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei;

8. O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pelo Departamento de Tecnologia;

9. Os colaboradores não poderão em hipótese alguma utilizar os recursos da Onze MC para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;

10. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

11. Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

12. Não serão permitidos os acessos a sites de compartilhamento de arquivos que não seja o autorizado e utilizado de forma corporativa pela Onze MC;

13. Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de by-pass de firewall;

14. Os arquivos inerentes à Onze MC, obrigatoriamente, deverão ser armazenados nos recursos disponibilizados e informados por cada responsável de área. É proibido armazenar estes tipos de arquivos em equipamentos pessoais;

15. Não é permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;

16. São gerados relatórios periódicos de sites e downloads acessados por usuário para análise de tráfego.

A Senha é forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra. O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

1. A senha é pessoal e intransferível, sendo expressamente proibida a divulgação ou empréstimo, devendo a mesma, ser imediatamente alterada no caso de suspeita de sua divulgação;

2. A senha inicial será fornecida ao próprio colaborador pelo seu gestor, pessoalmente. Não poderão ser fornecidas de qualquer outra forma que não assegure a identidade do colaborador;

3. É proibido o compartilhamento de contas de usuários (login);

4. As senhas não devem ser anotadas em papéis físicos;

5. As senhas deverão seguir os seguintes pré-requisitos:

- Tamanho mínimo de 8 caracteres

- Ter letras maiúsculas, minúsculas, números e caracteres especiais

- Não devem ser baseadas em informações pessoais (aniversário, nome do cônjugue, etc)

6. A conta do usuário será imediatamente cancelada nas seguintes situações:

- Desligamento do colaborador

- Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação

As Estações de Trabalho serão disponibilizadas operacionais de forma que o colaborador consiga realizar suas entregas e não tenham suas atividades prejudicadas. Algumas medidas de segurança serão tomadas, sendo:

1. É de responsabilidade do colaborador do equipamento zelar por ele, mantendo-o em boas condições;

2. Não é permitido personalizar o equipamento por adesivos, fotos, raspar e tirar a etiqueta de patrimônio;

3. É expressamente proibido a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o computador deverá ser encaminhado para a Equipe de Tecnologia;

4. É proibida a instalação de softwares que não sejam homologados pela Onze MC;

5. As estações de trabalho devem permanecer bloqueadas (logoff) nos períodos de ausência do colaborador;

6. Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados na plataforma corporativa, o qual possui rotinas de backup e controle de acesso adequado;

7. Todos os documentos relacionados à trabalho, deverão ser armazenados na plataforma corporativa (servidor de rede), nunca no disco local da máquina.

**7. CONFORMIDADE E EXECUÇÃO**

A violação desta Política pode causar danos à reputação da Onze MC ou levar a uma ação legal. Assim, o descumprimento desta Política, seja intencional ou não, será levado muito a sério.

O Gestor de TI e Segurança da Informação está autorizado à fazer cumprir as políticas aprovadas em cooperação com o Departamento de Recursos Humanos, o Departamento Jurídico e outras funções da empresa, conforme necessário.

Os colaboradores que violarem esta Política podem estar sujeitos a ações disciplinares, incluindo demissão. Para obter informações sobre o processo disciplinar da Onze MC, os colaboradores devem consultar os procedimentos e diretrizes disciplinares de Recursos Humanos aplicáveis.

Uma violação desta Política por fornecedores de serviços para a Onze MC ou qualquer outro usuário autorizado da área de tecnologia não empregado pela Onze MC pode resultar na rescisão de seu contrato com a Onze MC, rescisão do relacionamento entre a Onze MC e a empresa para a qual trabalham , ou rescisão do acesso. Além disso, a Onze MC pode optar por tomar medidas legais.

Colaboradores ou agentes de clientes ou colaboradores ou agentes de parceiros que tenham acesso aos dados armazenados na Onze MC e que violem a Política de Uso Adequado e quaisquer requisitos especiais de segurança e privacidade negociados em contratos podem perder seus privilégios de acesso; outras ações entre a Onze MC e o Cliente ou o Afiliado / Parceiro dependem dos acordos legais em vigor.

Qualquer colaborador que seja solicitado a realizar uma atividade que acredita estar em violação desta política deve levantar a questão, verbalmente ou por escrito, ao seu gerente, ao Gestor de TI e Segurança da Informação à algum outro membro da equipe de Segurança da Informação ou ao Departamento de Recursos Humanos o mais rápido possível. Qualquer usuário não colaborador que for solicitado a realizar uma atividade que acredita estar em violação a esta política deve levar o assunto, por escrito ou verbalmente, ao Gestor de TI e Segurança da Informação à um membro do Grupo de Risco e Segurança da Informação.

Transição para conformidade

Quando os sistemas, processos ou práticas são anteriores às versões recém-publicadas de políticas e padrões e não podem, portanto, estar em conformidade, o indivíduo responsável por cumprir a política (por exemplo, o proprietário do ativo) deve fornecer ao Gestor de TI e Segurança da Informação plano para alcançar a conformidade ou deve buscar um exceção de política.

**8. EXCEÇÕES**

Quando sistemas, processos ou práticas não cumprem ou não se espera que cumpram essas políticas, o indivíduo responsável deve solicitar a aprovação de uma exceção, deve identificar a duração da exceção proposta e deve fornecer um plano para atingir a conformidade. As exceções são aprovadas pelo Gestor de TI e Segurança da Informação, que pode delegar a aprovação ao profissional qualificado dependendo da magnitude do risco relacionado.

O aprovador da exceção deve considerar os riscos que podem ser apresentados à Onze MC por esta exceção e os atrasos resultantes no cumprimento da política.

**APÊNDICE I – SEGURANÇA DA INFORMAÇÃO E GESTÃO DE RISCO**

A Onze MC deve, por meio do Gestor de TI e Segurança da Informação, desenvolve e opera um Programa que deve incluir, mas não pode estar limitado às seguintes atividades:

• Avaliar os riscos de perda de confidencialidade, integridade e disponibilidade de tecnologia e dados da Onze MC, e orientar o tratamento de risco consistente com a Alta Administração;

• Desenvolver e manter as políticas necessárias para proteger a tecnologia e dados da Onze MC, equilibrando risco, custo e necessidades de negócios. As políticas e padrões entrarão em vigor mediante aprovação pela Alta Administração;

• Implementar padrões, controles, processos, práticas, comunicações, ferramentas e tecnologias necessárias para implementar as políticas;

• Adquirir as habilidades necessárias ou os serviços de terceiros necessários para implementar as políticas;

• Educar desenvolvedores de software, arquitetos de sistema, proprietários de dados, guardiões de dados, administradores de rede e sistema e usuários para garantir a consciência do risco, a consciência das boas práticas de segurança e a consciência dos requisitos de conformidade da política;

• Assegurar que os clientes, fornecedores e parceiros estejam cientes de suas responsabilidades para atender aos elementos apropriados das políticas de segurança da informação Onze MC, por meio de contratos e comunicações relacionadas;

• Faça cumprir a conformidade;

• Medir a conformidade e a eficácia das políticas, padrões e práticas e sua implementação e usar essas medidas para melhorar continuamente o programa de privacidade de segurança;

• Manter a consciência das ameaças emergentes à segurança da informação e incorporar no programa, métodos e tecnologias novos e úteis que mitiguem os riscos relacionados;

• Revisar o Programa como um todo, para garantir que ele atenda aos objetivos de segurança e conformidade da empresa, do cliente e de outras partes interessadas e equilibre a redução de riscos, custos e necessidades de negócios;

• Onde as condições técnicas, operacionais e comerciais locais o justifiquem, o Gestor de TI e Segurança da Informação trabalhar para adaptar o programa às circunstâncias locais.

APÊNDICE II – CONTROLE DE DOCUMENTO

Aprovação

Documento criado em 23/11/2020

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Aprovador | Cargo | Departamento | Revisado por | Data Revisão | Versão |
| Silvia Bussab | DPO / Gestora Adm/Fin | Administrativo / Financeiro | Rodrigo Dias / Silvia Bussab / Gustavo Iori | 27/01/2022 | 1.1 |
| Gustavo Iori | Gestor de TI e SI | TI e SI | Silvia Bussab | 23/11/2020 | 1.0 |
| Silvia Bussab | Gestora Adm/Fin | Administrativo / Financeiro | Paula Batiatto | 24/11/2020 | 1.0 |
| Paula Battiato | Diretora Executiva | Alta Administração |  | 26/11/2020 | 1.0 |